

DEPARTMENT OF THE NAVY  
Office of the Secretary  
Washington, D.C. 20350

SECNAVINST 3820.2D  
Op-009P  
20 August 1980

w/ch 1 26MR97

**SECNAV INSTRUCTION 3820.2D**

**From:** Secretary of the Navy  
**To:** All Ships and Stations

**Subj:** Investigative and counterintelligence collection and retention guidelines pertaining to the Department of the Navy

**Ref:** (a) DOD Directive 5240.1 of 30 Nov 79, Activities of DOD Intelligence Components that Affect U.S. Persons (NOTAL)  
(b) SECNAVINST 5520.3  
(c) SECNAVINST 12732.1 (NOTAL)  
(d) OPNAVINST 5510.1F  
(e) SECNAVINST 5212.5B  
(f) Guidelines of Archivist of the U.S. (NOTAL)

**Encl:** (1) DOD Directive 5200.26 of 12 Jun 79  
(2) DOD Directive 5200.27 of 7 Jan 80

**1. Purpose.** To implement within the Department of the Navy (DON) the Defense Investigative Program (DIP), and to set forth related policies concerning the collection and retention of information regarding persons and organizations not affiliated with the Department of Defense (DOD). This is a complete revision of this instruction to simplify its provisions and to implement a revision of DOD guidelines which now excludes DOD intelligence components from these collection and retention requirements.

**2. Cancellation.** SECNAV Instruction 3820.2C

**3. Scope**

a. Enclosure (1) assigns administrative and functional responsibilities for the DIP and applies to all DON investigative and related counterintelligence activities defined therein. Specifically excluded from its coverage are pretrial investigations required by the Uniform Code of Military Justice, criminal investigations (except when they involve functions identified in subsection C.1 of enclosure (1)), and activities incident to the acquisition of foreign intelligence or to the activities involved in insuring communications security

b. Enclosure (2) provides the DIP general policy, limitations, procedures, and operational guidance pertaining to the collection, processing, storage and dissemination of information concerning persons and organizations not affiliated with the DOD. It does not apply to DOD intelligence components which are defined in and regulated by reference (a). The provisions of enclosure (2) encompass the acquisition of information concerning the activities of non-DOD affiliated persons and organizations within the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions; and non-DOD affiliated U.S. citizens anywhere in the world. Persons or organizations are considered DOD affiliated if they are:

(1) Employed by or contracting with DOD or by any activity under the jurisdiction of DOD, whether on a full-time, part-time, or consultive basis;

(2) Members of the Armed Forces on active duty, national guard members, those in a reserve status or in a retired status;

(3) Residing on, have authorized official access to, or conducting or operating any business or other function at any DOD installation or facility;

(4) Having authorized access to defense information;

(5) Participating in other authorized DOD Programs; or

(6) Applying for or being considered for any status described above in subparagraphs (1) through (5).

**4. Responsibilities**

a. The Under Secretary of the Navy is assigned responsibility for DIP activities within the DON. Additionally, the Under Secretary of the Navy is assigned the primary supporting role to the Secretary of the Navy in carrying out the functions enumerated in subsections E.2.b through d of enclosure (1).

**SECNAVINST 3820.2D**  
**20 August 1980**

b. Reference (b) established within the DON the respective responsibilities of the Naval Investigative Service (NAVINSERV) and Marine Corps and command investigative units. The primary responsibility for conducting the activities permitted by enclosure (2) is vested in the NAVINSERV.

**5. Guidance**

a. Commands having requirements for information concerning persons or organizations not affiliated with the DOD shall seek assistance pursuant to the provisions of references (b), (c), or (d), as appropriate.

b. The primary collector of such information within the DON is the NAVINSERV. The NAVINSERV is the only DON element authorized to conduct the activities permitted by subsections E.5 and 6 of enclosure (2). The NAVINSERV shall effect this function in strict compliance with reference (a), where applicable.

c. Under emergency conditions local commanders, without prior approval of higher authority, may authorize the activities regulated by subsection E.6 of enclosure (2). The assistance of the NAVINSERV shall be requested when the local commander perceives a direct and immediate threat to DOD functions or property; time precludes the obtaining of prior approval by higher authority; and non-DOD collection agencies are unable to fulfill Navy requirements. When a local commander authorizes such a collection effort, an immediate report shall be made by that commander to the Chief of Naval Operations (CNO) or the Commandant of the Marine Corps (CMC), as appropriate. Copies of such reports shall be immediately provided by the local commander to Director, NAVINSERV, the local NAVINSERV component, and appropriate authorities within the

commander's chain of command. A report to the Under Secretary of the Navy shall be made immediately by the CNO or CMC, as appropriate.

**6. Records Retention**

a. Subsection F.4 of enclosure (2) requires that all information within the purview of that directive shall be destroyed within 90 days unless its retention is required by law or unless retention is specifically authorized under criteria established by the Secretary of Defense, or his designee.

b. To assure compliance with this provision, the following retention procedures shall be followed within the DON with respect to DIP information relating to non-DOD affiliated persons or organizations except as specifically excluded in subparagraphs 3a and 3b above.

(1) The NAVINSERV will retain such records in accordance with references (e) and (f) and applicable laws and directives. When NAVINSERV disseminates records containing such information to other DON elements the records shall contain retention guidelines.

(2) Other DON elements shall not retain such records longer than 90 days or, in the case of NAVINSERV disseminated records, the date specified by NAVINSERV. Any exception shall require the approval of the Under Secretary of the Navy.

**7. Report.** Symbol SECNAV 3820-1 (MIN:CONSIDERED) is assigned to the reporting requirement of subparagraph 5c. This report is approved for 15 years only from the date of this directive.

**EDWARD HIDALGO**

**Distribution:**  
**SNDL Parts 1 and 2**  
**MARCORPS L5/L10**

**Chief of Naval Operations**  
**OP-09B15C**  
**Wash., D.C. 20350 (200 copies)**

**Stocked:**  
**CO, NAVPUBFORMCEN**  
**5801 Tabor Ave.**  
**Phila., PA 19120 (600 copies)**

20 AUG 1980

June 12, 1979  
NUMBER 5200.26**Department of Defense Directive** JSD(P)**SUBJECT** Defense Investigative Program

References: (a) DoD Directive 5200.26, "Defense Investigative Program," February 17, 1971 (hereby canceled)  
(b) DoD Directive 5130.2, "Director of Policy Review," June 16, 1977

**A. REISSUANCE AND PURPOSE**

This Directive reissues reference (a) which established a coordinated Defense Investigative Program within the Department of Defense and assigned functions and responsibilities for the administration of the program.

**B. APPLICABILITY AND SCOPE**

The provisions of this Directive apply to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, and the Defense Agencies (hereinafter referred to as the "DoD Components"), and cover investigative activities as defined herein.

**C. DEFINITION**

1. The Defense Investigative Program, as used in this Directive, includes those investigative and related counterintelligence activities which:

- a. Safeguard defense information.
- b. Protect DoD personnel against subversion.
- c. Protect DoD functions and property, including facilities which have classified defense contracts or which have been designated officially as key defense facilities.
- d. Conduct personnel security investigations for DoD personnel and contractor employees under the Defense Industrial Security Program.

Enclosure (1)

e. Conduct counterintelligence surveys, services, and inspections.

f. Conduct authorized investigative activities in connection with civil disturbances within the United States, the District of Columbia, the Commonwealth of Puerto Rico, and United States' territories and possessions.

2. This Directive does not apply to pretrial investigations required by the Uniform Code of Military Justice, criminal investigations other than those involving the functions enumerated above, and activities incident to the acquisition of foreign intelligence or to the activities involved in ensuring communications security.

#### D. POLICY

It is the policy of the Department of Defense to establish standards, criteria, and operational guidance under senior civilian cognizance and control for a centralized Defense Investigative Program that protects national security interests while ensuring that the constitutional civil and private rights of individuals and organizations are protected.

#### E. RESPONSIBILITIES AND FUNCTIONS

1. The Deputy Under Secretary of Defense for Policy Review (DUSD(PR)) shall act for the Secretary of Defense in the direction, management, and review of the Defense Investigative Program. In carrying out this responsibility, the DUSD(PR) shall:

a. Establish policies for the conduct of the Defense Investigative Program.

b. Provide for program management of all counterintelligence and investigative resources within the Department of Defense.

c. Conduct or provide for inspections of program activities and monitor program accomplishments.

d. Assign tasks to DoD Components to accomplish Defense Investigative Program objectives.

e. Review programs, budgets, and financial plans which support Defense Investigative Program activities.

f. Provide representation on boards and committees of the Defense Investigative Program.

Jun 12, 79  
5200.26

g. Coordinate and supervise relations of DoD Components with other Government agencies on Defense Investigative Program matters.

h. Perform other functions of the Defense Investigative Program which may be assigned by the Secretary of Defense.

2. The Secretaries of the Military Departments shall:

a. Assign the Under Secretary or an Assistant Secretary to be responsible for the conduct of Defense Investigative Program activities.


b. Provide management, review, and inspection of the investigative activities of their Departments, and forward a consolidated report of inspections to the DUSD(PR) annually.

c. Recommend to the DUSD(PR) changes to prescribed policies, procedures, or practices in the Defense Investigative Program.

d. Assist as required in the conduct of inspections of Defense Investigative Program activities undertaken by the DUSD(PR).

F. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing documents to the DUSD(PR) within 60 days.

  
C. W. Duncan, Jr.  
Deputy Secretary of Defense

40 AUG 1980

January 7, 1980  
NUMBER 5200.27**Department of Defense Directive**

USDP

SUBJECT: Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

References: (a) DoD Directive 5200.27, subject as above, December 8, 1975 (hereby canceled)  
(b) DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," November 30, 1979

**A. REISSUANCE AND PURPOSE**

This Directive reissues reference (a) to establish for the Defense Investigative Program general policy, limitations, procedures, and operational guidance pertaining to the collecting, processing, storing, and disseminating of information concerning persons and organizations not affiliated with the Department of Defense.

**B. APPLICABILITY AND SCOPE**

1. Except as provided by subsection B.3., below, this Directive is applicable to the Office of the Secretary of Defense, Military Departments, Office of the Joint Chiefs of Staff, Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").

2. The provisions of this Directive encompass the acquisition of information concerning the activities of:

a. Persons and organizations, not affiliated with the Department of Defense, within the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions; and

b. Non-DoD-affiliated U.S. citizens anywhere in the world.

3. This Directive is not applicable to DoD intelligence components as defined by DoD Directive 5240.1 (reference (b)).

4. Authority to act for the Secretary of Defense in matters in this Directive which require specific approval are delineated in enclosure 1.

Enclosure (2)

### C. POLICY

1. Department of Defense policy prohibits collecting, reporting, processing, or storing information on individuals or organizations not affiliated with the Department of Defense, except in those limited circumstances where such information is essential to the accomplishment of the Department of Defense missions outlined below.

2. Information-gathering activities shall be subject to overall civilian control, a high level of general supervision and frequent inspections at the field level.

3. Where collection activities are authorized to meet an essential requirement for information, maximum reliance shall be placed upon domestic civilian investigative agencies, Federal, State and local.

4. In applying the criteria for the acquisition and retention of information established pursuant to this Directive, due consideration shall be given to the need to protect DoD functions and property in the different circumstances existing in geographic areas outside the United States. Relevant factors include:

- a. The level of disruptive activity against U.S. forces;
- b. The competence of host country investigative agencies;
- c. The degree to which U.S. military and host country agencies exchange investigative information;
- d. The absence of other U.S. investigative capabilities; and
- e. The unique and vulnerable position of U.S. forces abroad.

### D. AUTHORIZED ACTIVITIES

DoD Components are authorized to gather information essential to the accomplishment of the following defense missions:

1. Protection of DoD Functions and Property. Information may be acquired about activities threatening defense military and civilian personnel and defense activities and installations, including vessels, aircraft, communications equipment, and supplies. Only the following types of activities justify acquisition of information under the authority of this subsection:

a. Subversion of loyalty, discipline, or morale of DoD military or civilian personnel by actively encouraging violation of law, disobedience of lawful order or regulation, or disruption of military activities.

b. Theft of arms, ammunition, or equipment, or destruction or sabotage of facilities, equipment, or records belonging to DoD units or installations.

c. Acts jeopardizing the security of DoD elements or operations or compromising classified defense information by unauthorized disclosure or by espionage.

d. Unauthorized demonstrations on active or reserve DoD installations.

e. Direct threats to DoD military or civilian personnel in connection with their official duties or to other persons who have been authorized protection by DoD resources.

f. Activities endangering facilities which have classified defense contracts or which have been officially designated as key defense facilities.

g. Crimes for which DoD has responsibility for investigating or prosecuting.

2. Personnel Security. Investigations may be conducted in relation to the following categories of persons:

a. Members of the Armed Forces, including retired personnel, members of the Reserve Components, and applicants for commission or enlistment.

b. DoD civilian personnel and applicants for such status.

c. Persons having need for access to official information requiring protection in the interest of national defense under the Department of Defense Industrial Security Program or being considered for participation in other authorized Department of Defense programs.

3. Operations Related to Civil Disturbance. The Attorney General is the chief civilian officer in charge of coordinating all Federal Government activities relating to civil disturbances. Upon specific prior authorization of the Secretary of Defense or his designee, information may be acquired which is essential to meet operational requirements flowing from the mission assigned to the Department of Defense to assist civil authorities in dealing with civil disturbances. Such authorization will only be granted when there is a distinct threat of a civil disturbance exceeding the law enforcement capabilities of State and local authorities.

#### E. PROHIBITED ACTIVITIES

1. The acquisition of information on individuals or organizations not affiliated with the Department of Defense will be restricted to that which is essential to the accomplishment of assigned Department of Defense missions under this Directive.

2. No information shall be acquired about a person or organization solely because of lawful advocacy of measures in opposition to Government policy.



3. There shall be no physical or electronic surveillance of Federal, State, or local officials or of candidates for such offices.

4. There shall be no electronic surveillance of any individual or organization except as authorized by law.

5. There shall be no covert or otherwise deceptive surveillance or penetration of civilian organizations unless specifically authorized by the Secretary of Defense, or his designee.

6. No DoD personnel will be assigned to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information, the collection of which is authorized by this Directive without specific prior approval by the Secretary of Defense, or his designee. An exception to this policy may be made by the local commander concerned, or higher authority, when, in his judgment, the threat is direct and immediate and time precludes obtaining prior approval. In each such case a report will be made immediately to the Secretary of Defense, or his designee.

7. No computerized data banks shall be maintained relating to individuals or organizations not affiliated with the Department of Defense, unless authorized by the Secretary of Defense, or his designee.

#### F. OPERATIONAL GUIDANCE

1. Nothing in this Directive shall be construed to prohibit the prompt reporting to law enforcement agencies of any information indicating the existence of a threat to life or property, or the violation of law, nor to prohibit keeping a record of such a report.

2. Nothing in this Directive shall be construed to restrict the direct acquisition by overt means of the following information:

a. Listings of Federal, State, and local officials who have official responsibilities related to the control of civil disturbances. Such listings may be maintained currently.

b. Physical data on vital public or private installations, facilities, highways, and utilities, as appropriate, to carry out a mission assigned by this Directive.

3. Access to information obtained under the provisions of this Directive shall be restricted to governmental agencies which require such information in the execution of their duties.

4. Information within the purview of this Directive, regardless of when acquired, shall be destroyed within 90 days unless its retention is required by law or unless its retention is specifically authorized under criteria established by the Secretary of Defense, or his designee.

January 7, 1980  
5200.27

5. This Directive does not abrogate any provision of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, April 5, 1979, nor preclude the collection of information required by Federal statute or Executive Order.

G. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing regulations to the Deputy Under Secretary of Defense (Policy Review) within 120 days.



W. Graham Claytor, Jr.  
Deputy Secretary of Defense

Enclosure - 1  
Delegation of Authority

DELEGATION OF AUTHORITY

A. The Secretary of the Army is designated to authorize those activities delineated in subsection D.3., basic Directive. This authority may not be further delegated to other than the Under Secretary of the Army.

B. The Deputy Under Secretary of Defense (Policy Review) (DUSD(PR)) is designated to authorize those activities delineated in subsection E.5., basic Directive, within the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions. This authority may not be delegated. The investigating DoD Component, prior to requesting approval for authorizations under this provision, shall coordinate prospective activities with the Federal Bureau of Investigation.

C. The DUSD(PR) and the Secretaries of the Military Departments are designated to authorize those activities (delineated in subsection E.5., basic Directive) abroad<sup>1</sup> when membership of the civilian organization is reasonably expected to include a significant number of non-DoD-affiliated U.S. citizens. This authority may not be further delegated to other than the Under Secretaries of the Military Departments. When the Military Department Secretary or Under Secretary exercises this delegation of authority, the DUSD(PR) shall be advised promptly.

D. The Secretaries of the Military Departments are designated to authorize in their Departments those activities delineated in subsection E.6., basic Directive, within the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions. This authority may not be further delegated to other than the Under Secretaries of the Military Departments.

E. The Secretaries of the Military Departments are designated to authorize in their Departments those activities (delineated in subsection E.6., basic Directive) abroad<sup>1</sup> when a significant number of non-DoD-affiliated U.S. citizens are expected to be present. This authority may be further delegated, in writing, as circumstances warrant, to an authorized designee. The DUSD(PR) will be notified immediately of such further delegations of authority. When the Secretary or Under Secretary of a Military Department or his designee exercises this delegated authority, the DUSD(PR) shall be advised promptly.

F. The DUSD(PR) is designated to authorize those activities delineated in subsections E.7. and F.4., basic Directive. These authorities may not be further delegated.

<sup>1</sup>"Abroad" means "outside the United States, its territories and possessions."